DISCIPLINE: Host Protection

Discipline Roadmap for: Anti-Spyware

DOMAIN: SECURITY

Current	2 Years	5 Years

Baseline Environment

Host-based

- Websense
- McAfee
- LavaSoft
- Microsoft
- Sunbelt
- Symantec
- PC Tools (unmanaged)
- Spybot Search and Destroy

Network-based

- LavaSoft
- Barracuda
- Intrusion Inc. (SpySnare)
- SonicWALL

Root Kit Defense

- Microsoft
- Backlight Defender

Tactical Deployment

Strategic Direction

Market watch for consolidated products.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

This market is poised for significant consolidation.

Implications and Dependencies

- Centralized management and administration of host-based clients.
- It is highly recommended that multiple products be used in concert in order to create an in-depth defense since not all products defend equally.

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.

DISCIPLINE: Host Protection

Discipline Roadmap for: Anti-Spyware

- **Discipline Boundaries:**
  - Spyware is a broad category of software designed to subvert a computer’s operation for the benefit of a third party, without the informed consent of the owner. Spyware may be malicious in nature, intending to collect financial information for identify-theft or it can be relatively benign, originating form legitimate companies for the intended purpose of advertising. Anti-spyware is software that is designed to remove or block spyware.
- **Discipline Standards:**
  - Currently, there are no anti-spyware specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - Entities should consider restricting intentional downloading and installation of programs.
  - Entities should consider providing training to educate users in areas, such as:
    - Understanding of End User License Agreement (EULA), since often times agreements to install spyware are included in the fine print.
    - Proper response to pop-up windows.
    - Recognition of spyware symptoms.
    - Awareness of suspicious emails and “free” software.
  - Entities should consider tightening browser security, e.g. disabling Active X.
  - Entities should consider installing pop-up blockers.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007